Managing Personally Identifiable Information

From Reaction to Prevention

Executive Office of Administration and Finance
Information Technology Division

November 18, 2008

Dan Walsh, CISSP
CSO
Commonwealth of Massachusetts
Information Technology Division

Tipping Point Passed

Identity theft is now passing drug trafficking as the number one crime in the nation

U.S. Department of Justice

http://www.idtheftcenter.org/artman2/publish/m_facts/Facts_and_Statistics.shtml

Massachusetts ranks 22nd out of 50 states:
63.7 victims per 100,000 Population

http://www.identitytheftsecurity.com/stats.shtml#2006stats

Reactive Models

Breach Notification

44 states have since enacted legislation which Requires notification of Security breaches involving Personal information

National conference of state legislatures
http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm

To-Date Reporting

Sources

Over 10 months since the new identity theft law took effect Office of Consumer Affairs and Business Regulation has received 318 notifications of such breaches

a. **274 were reported by businesses (86%)**
b. **23 by educational institutions (8%)**
c. **17 by state government (5%)**
d. **4 by not-for-profits (1%)**

http://www.mass.gov/?pageID=ocahomepage&L=1&L0=Home&sid=Eoca

To-Date Scenarios

- Corporate Espionage
- Extortion
- Organized Crime
- State-Sponsored Terrorism
- Internal Unauthorized Access
- Errors
- Lost Equipment

2007 statistics[1]

$197

Cost to companies per compromised record

$6.3 Million

Average cost per data breach "incident"

40%

% of breaches where the responsibility was with Outsourcers, contractors, consultants and business partners

235 Million

TOTAL number of records containing sensitive personal information involved in security breaches in the U.S. since 2005

[1] Ponemon Institute, Privacy Rights Clearinghouse, 2007

Governance
Enterprise Security Board (ESB) 2001

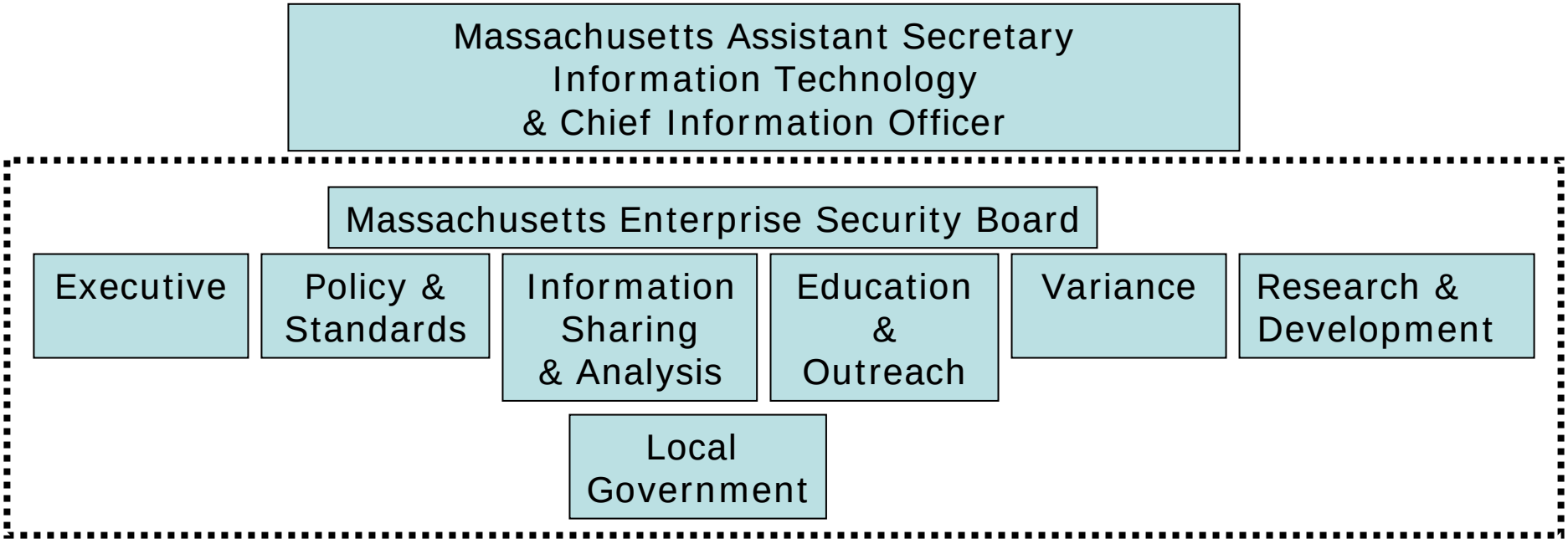
Based on the work & recommendations of ESB, ITD has issued enterprise security policies addressing

- Attack intrusion notification
- **Cybercrime and security incidents**
- **Electronic messaging communications security**
- **Information security policy**
- **Data classification**
- **E-government apps public access policy and standards**
- Remote access
- Wireless implementations

Become More Proactive
EO504 Meets Governance

CIO shall determine members and makeup of ESB, but membership shall be drawn from

- State employees from Executive Department
- Experience in IT, privacy, and security
- Representatives from Judicial and Legislative Branches
- Other constitutional offices
- Quasi-public authorities



EO 504 Paving the Way
What's New?[2]

- **Requirement for agency security officers (addressing both Privacy and Security) and written information security plans (including ESPs)**
- **Requirement for agency at least annual ESP self audit, sent to ITD**
- **Additional ANF/ITD authority over agency IT spending based on agency compliance with ESP self audit**
- **Focus on data destruction (also required under G.L. c. 93I)**
- **Agencies must give full cooperation, and information, to ITD**

[2] Source: ITD General Counsel's Office